CA TPX™ Session Management

Installation Guide

Release 5.4

CA Technologies Product References

This document references the following CA Technologies products:

- CA TPX™ Session Management (CA TPX)
- CA STX™ (CA STX)
- CA ACF2™ Security (CA ACF2)
- CA Top Secret® Security (CA Top Secret)
- CA IDMS™ Database (CA IDMS Database)
- CA IDMS™/DC Database (CA IDMS/DC Database)
- CA 7® Job Management (CA 7)
- CA Remote Console™ (CA Remote)
- CA TCPaccess™ Telnet Server (CA TCPaccess Telnet Server)
- CA Vman™ (CA Vman)
- CA Common Services™ Resource Initialization Manager (CAIRIM)
- CA MII Data Sharing (CA MII)
- CA Mainframe Software Manager (CA MSM)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Overview

CA TPX (Terminal Productivity Executive) is a VTAM session management tool that provides a consistent, secure point of entry to multiple, simultaneous mainframe applications. This chapter describes the audience for this guide and provides an overview of CA TPX functions.

CA TPX allows you to run multiple application sessions on a 3270-type terminal (real or emulated) in a VTAM environment. The product manages these sessions. As a user, you have simultaneous access to a number of applications and can toggle between application sessions without having to log off one application and log on to another. You can access all the applications you need from one physical terminal.

For users who access the mainframe through a PC-based 3270-type terminal emulator, the TCPaccess Telnet Server provides a fast, direct Telnet connection to CA TPX.

This section contains the following topics:

Audience

The system programming group is usually responsible for software product installation and maintenance because of their SMP/E (System Modification Program Extended) knowledge. This guide assumes a working knowledge of the SMP/E facility and its processes.

This guide provides basic standalone SMP/E install and maintenance instructions. For the knowledgeable SMP/E user, there is enough information provided in this guide, and the generated JCL and control statements, to allow integration with any site-specific SMP/E standards. For the SMP/E novice, this guide should provide enough of the basic information and concepts you need to complete the basic SMP/E installation process.

How the Installation Process Works

CA Technologies has standardized product installations across all mainframe products. Installation uses the following process:

- Acquisition—Transports the software to your z/OS system.
- Installation using SMP/E—Optionally creates a CSI environment and runs the RECEIVE, APPLY and ACCEPT steps. The software is untailored.
- Deployment—Copies the target libraries to another system or LPAR.
- Configuration—Creates customized load modules, bringing the software to an executable state.

CA MSM provides a web-based interface to make the standardized installation process easier. Using CA MSM, someone with limited knowledge of JCL and SMP/E can install a product.

Note: If you do not have CA MSM, you can download it from the Download Center at the CA Support Online website. Follow the installation instructions in the CA Mainframe Software Manager documentation bookshelf on the CA Mainframe Software Manager product page. The standardized installation process can also be completed manually.

To install your product, do the following tasks:

1. Prepare for the installation by confirming that your site meets all installation requirements (see page 11).
2. Acquire the product using one of the following methods:
   - CA MSM
   - Pax-Enhanced Electronic Software Delivery (ESD)
   - Order a DVD.
3. Install the product based on your acquisition method.
4. Install the CA Common Services using the pax files that contain the CA Common Services you need at your site.

   All sites should install all CA Common Services contained in the Required CA Common Service bundle.
5. Apply maintenance, if applicable.
6. Deploy your target libraries.
7. Configure your product.

Chapter 2: Preparing for Installation

This section describes what you need to know and do before you install the product.

This section contains the following topics:

CA Common Services Requirements

CA TPX uses the CCS component CAIRIM, the Resource Initialization Manager, for product license authorization.

CAIRIM is a common component whose features and functions are shared by many CA z/OS products. This component prepares your operating system environment for your CA products and components and executes them.

CAIRIM routines are grouped under CA z/OS Dynamic Service Code S910. For further details about the features and associated utilities of CAIRIM, review the CCS for z/OS documentation.

CA Health Checker

Provides a simple and consistent method for CA products to create health checks to run under the IBM Health Checker for z/OS. The IBM Health Checker for z/OS helps you identify potential problems in your z/OS environment by checking system or product parameters and system status against recommended settings. CA has joined other vendors in creating checks for CA z/OS products. CA TPX health checks are automatically activated on the target system when the product is started on a system where the following components are installed and configured:

- CA Health Checker Common Service
- IBM Health Checker for z/OS

For more information on installing the CA Health Checker Common Service, see the *CA Common Service Installation Guide.*

For more information about the IBM Health Checker for z/OS, see the *IBM Health Checker for z/OS User Guide*.

CA LMP

This product requires CA LMP (License Management Program) to initialize correctly. CA LMP also provides a standardized and automated approach to the tracking of licensed software.

CA LMP is provided as an integral part of CAIRIM. When a currently supported version of CAIRIM has been installed, assistance is available to you for all CA LMP-supported products.

Specify the LMP Code

You must add the CA LMP Execution Key provided on the Key Certificate to the CAIRIM parameters to ensure proper initialization of this product.

To define a CA LMP Execution Key to the CAIRIM parameters, modify member KEYS in CAI.PPOPTION.

The statement structure for member KEYS is:

```
PROD(pp) DATE (ddmmmyy) CPU (tttt-mmmm/ssssss)
LMPCODE (kkkkkkkkkkkkkkkk)
```

CAIRIM Parameters

The CAIRIM parameter definitions are:

Parameter	Definition
pp	The two-character product code. This code agrees with the product code already in use by the CAIRIM initialization parameters for any earlier versions of this product (if applicable). This is required.
ddmmmyy	The CA LMP licensing agreement expiration date.
ttt-mmmm	The CPU type and model on which CA LMP is to run (for example, 3090-600). If the CPU type, model, or both require less than four characters, blank spaces are inserted for the unused characters. This is required.
ssssss	The serial number of the CPU on which CA LMP is to run. This is required.
kkkkkkkkkkkkkkkk	The execution key needed to run CA LMP. This CA LMP execution key is provided on the Key Certificate shipped with each CA LMP software solution.

Following is an example of a control statement for the CA LMP execution software parameter. The product code and execution key value will be different when you install this product at your site.

```
PROD(1B) DATE (27JUN03) CPU(3090-600 /370623)
LMPCODE(52H2K06130Z7RZD6)
```

For more information regarding the CA Common Services CAIRIM and its CA-LMP facility, see the *CA Common Services for z/OS Administration Guide*.

Other Requirements

The installation procedure involves loading the CA TPX installation data sets from the distribution media and customizing statements in these data sets for your site.

The administration facility, required for performing online administration, is installed automatically when you install this product.

Coupling Facility

Optionally define the Coupling Facility structure for use by CA TPX in the z/OS policy data set. This is required if multiple instances of CA TPX are to operate as a single VTAM generic resource.

Naming Conventions

The INSTALL data set that you use to install this product uses PREFIX execution parameters to set the values of the prefixes used in data set names. If you choose to change this value, make sure you change it consistently throughout the installation procedure, and check that all parameters in the INSTALL data sets conform to the conventions at your site.

The examples in this guide use the original values for the application name, TPX. If you assign a different name, make appropriate changes consistently throughout the installation procedure.

Concurrent Releases

You can install this release of CA TPX and continue to use an older release in another SMP/E CSI environment. If you plan to continue to run a previous release, consider the following points:

- When installing into an existing SMP/E environment, this installation deletes previous releases in that environment.
- If you acquired your product from tape or with Pax-Enhanced ESD, select different target and distribution zones for your new release from where your current release is installed. The new zones use different libraries than your current release.

  Note: CA MSM installs into a new CSI by default.
- Define DDDEF entries in your new zones to point SMP/E to the proper libraries for installation. Ensure that they point to the new release libraries.

Chapter 3: Installing Your Product Using CA MSM

Use the procedures in this section to manage your product using CA MSM. Managing includes acquiring, installing, maintaining, and deploying products, setting system registries, and managing your CSIs. These procedures assume that you have already installed and configured CA MSM.

Note: If you do not have CA MSM, you can download it from the Download Center at the CA Support Online website. Follow the installation instructions in the CA Mainframe Software Manager documentation bookshelf on the CA Mainframe Software Manager product page.

When you have completed the procedures in this section, go to Configuring Your Product (see page 47).

This section contains the following topics:

These topics provide information to get you started managing your product using CA MSM. You can use the online help included in CA MSM to get additional information.

Before using these topics, you must already have CA MSM installed at your site. If you do not have CA MSM installed, you can download it from the Download Center at the CA Support Online website, which also contains links to the complete documentation for CA MSM.

How to Use CA MSM: Scenarios

Imagine that your organization has started using CA MSM to simplify the installation of CA Technologies products and unify their management. You have also licensed a new CA Technologies product. In addition, you have a number of existing SMP/E environments from previously installed CA Technologies products.

You can use the following scenarios to guide you through the process:

1. Acquire the new product (see page 16).
2. Install the new product (see page 17).

3. Maintain products already installed in your environment (see page 19).
4. Set up the CA MSM system registry (see page 20).
5. Deploy the product to your target systems (see page 22).
6. Configure the deployed product to your target systems (see page 23).

How to Acquire a Product

The *Product Acquisition Service (PAS)* facilitates the acquisition of mainframe products and the service for those products, such as program temporary fixes (PTFs). PAS retrieves information about products to which your site is entitled. Then it records these entitlements in a software inventory that is maintained on your driving system.

You can use the PAS component of CA MSM to acquire a CA Technologies product.

You perform the following high-level tasks to acquire a product using CA MSM:

1. Set up a CA Support Online account.

   To use CA MSM to acquire or download a product, you must have a CA Support Online account. If you do not have an account, you can create one on the CA Support Online website.

2. Determine the CA MSM URL for your site.

   To access CA MSM (see page 24), you require its URL. You can get the URL from your site CA MSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA MSM account with your credentials for the CA Support Online website. This account enables you to download product packages.

3. Log in to CA MSM and go to the Software Catalog page to locate the product that you want to manage.

   After you log in to CA MSM, you can see the products to which your organization is entitled on the Software Catalog tab.

   If you cannot find the product that you want to acquire, update the catalog. CA MSM refreshes the catalog through the CA Support Online website using the site IDs associated with your credentials for the CA Support Online website.

4. Download the product installation packages.

   After you find your product in the catalog, you can download the product installation packages.

   CA MSM downloads (acquires) the packages (including any maintenance packages) from the CA FTP site.

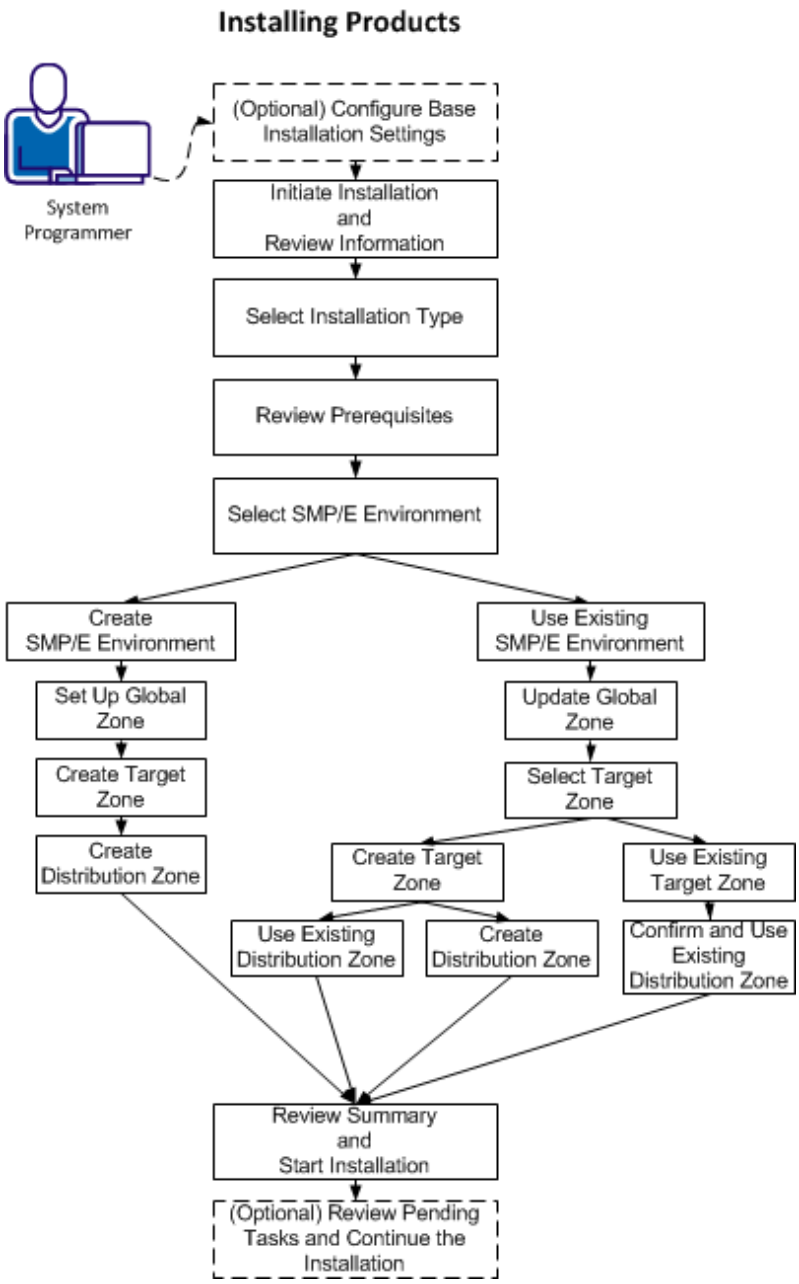
After the acquisition process completes, the product is ready for you to install or maintain.

How to Install a Product

The *Software Installation Service (SIS)* facilitates the installation and maintenance of mainframe products in the software inventory of the driving system. This facilitation includes browsing downloaded software packages, managing SMP/E consolidated software inventories on the driving system, and automating installation tasks.

You can use the SIS component of CA MSM to install a CA Technologies product.

You perform the following high-level tasks to install a product using CA MSM:



1. (Optional) Configure base installation settings.
2. Initiate product installation and review product information.
3. Select an installation type.
4. Review installation prerequisites if any are presented.

5. Take *one* of the following steps to select an SMP/E environment:
   - Create an SMP/E environment:
     a. Set up the global zone.
     b. Create a target zone.
     c. Create a distribution zone.
   - Use an existing SMP/E environment from your working set:
     a. Update the global zone.
     b. Set up the target zone: Either create a target zone or use an existing target zone.
     c. Set up the distribution zone: Either create a distribution zone or use an existing distribution zone.

     Note: If you install a product or its components into an existing target or distribution zone, older versions are deleted from the zone and associated data sets. We recommend that you use new target and distribution zones for this installation so that you can apply maintenance to your current version, if necessary.
6. Review the installation summary and start the installation.
7. (Optional) Review pending tasks for the SMP/E environment where you are installing your product. Continue the installation, if applicable.

After the installation process completes, check for and install available product maintenance. The product is ready for you to deploy. Sometimes there are other steps to perform manually outside of CA MSM before beginning the deployment process.

More information:

How to Maintain Existing Products (see page 19)

How to Maintain Existing Products

You can migrate existing SMP/E environments into CA MSM to maintain all your installed products in a unified way from a single web-based interface.

You can use CA MSM to maintain a CA Technologies product.

You perform the following high-level tasks to maintain a product using CA MSM:

1. Migrate the SMP/E environment to CA MSM to maintain an existing SMP/E environment in CA MSM.

   During the migration, CA MSM stores information about the SMP/E environment in the database.

2. Download the latest maintenance for the installed product releases from the Software Catalog tab.

   If you cannot find the required release, you can perform the following steps to download the maintenance:

   a. Add the release to the catalog manually.

   b. Update the release.

3. Apply the maintenance.

Note: You can also install maintenance to a particular SMP/E environment from the SMP/E Environments tab.

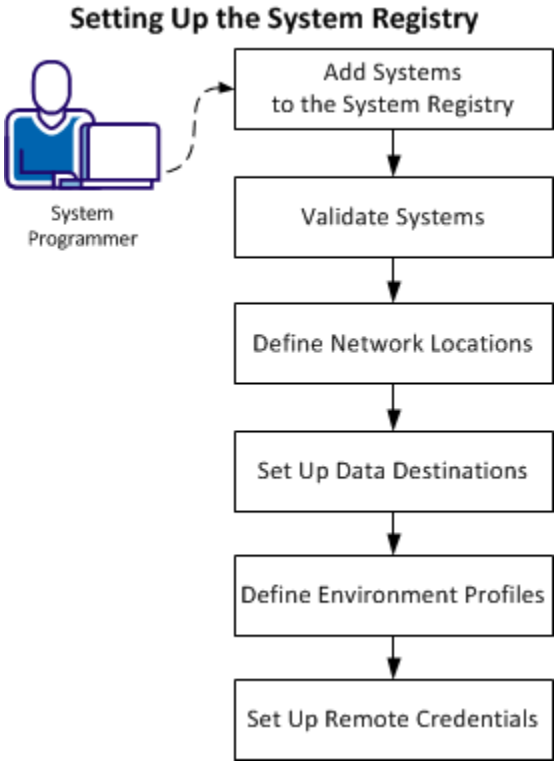
After the maintenance process completes, the product is ready for you to deploy. Sometimes there are other steps to perform manually outside of CA MSM before beginning the deployment process.

How to Set Up the System Registry

The *system registry* is a repository of variable data that all CA MSM managed products share. The system registry repository contains information about the systems that have been defined to CA MSM and selected as a target for deployments and configurations. You can create non-sysplex, sysplex, shared DASD cluster, and staging systems. You can maintain, validate, view, and delete a registered system and you can investigate a failed validation.

For each system that you register, there is one entry. Each entry consists of three categories of information: general, network locations, and data destinations.

You perform the following tasks to set up the system registry in CA MSM:



1. Add systems to the system registry.
2. Validate systems.
3. Define network locations.
4. Set up data destinations.
5. Define environment profiles.
6. Set up remote credentials.

Add and then validate each nonstaging system in the enterprise that you are deploying to, to the CA MSM system registry. You can only send a deployment to a validated system.

This process applies to each nonstaging system in your enterprise. For example, if you have five systems at your enterprise, then perform this process five times.

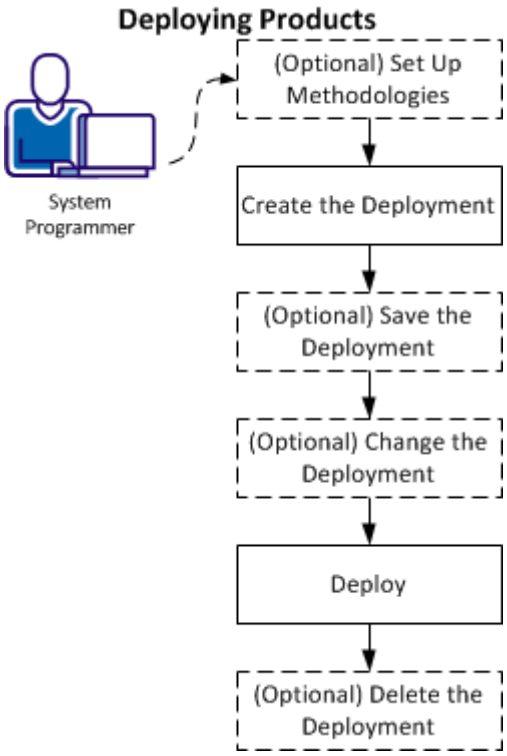
Note: After a system is validated, there is no need to validate it again. However, you can revalidate a system any time.

How to Deploy a Product

The *Software Deployment Service (SDS)* facilitates the mainframe product deployment from the software inventory of the driving system to the target system. This facilitation includes deploying installed products that are policy-driven with a set of appropriate transport mechanisms across a known topology.

You can use the SDS component of CA MSM to deploy a CA Technologies product that you have already acquired and installed.

You perform the following high-level tasks to deploy your products using CA MSM:



1. (Optional) Set up methodologies.

   Note: You can also set up methodologies when creating a deployment.

2. Create the deployment.
3. (Optional) Save the deployment for editing and deploying later.
4. (Optional) Change the deployment: Add and edit systems, products, custom data sets, and methodologies.

5. Deploy:
    a. Take a snapshot.
    b. Transmit to target.
    c. Deploy (unpack) to mainframe environment.
6. (Optional) Delete the deployment.

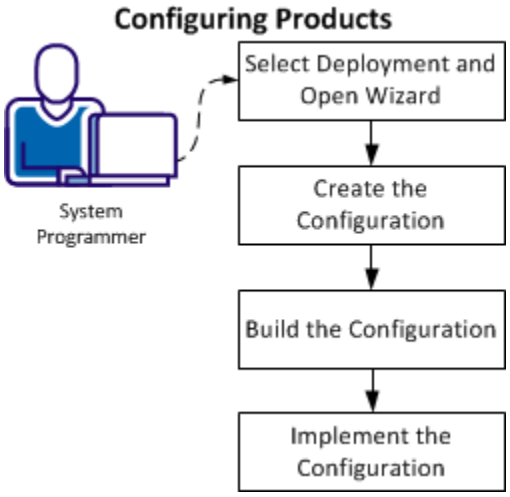
After the deployment process completes, the product is ready for you to configure. Sometimes there are other steps to perform manually outside of CA MSM before beginning the configuration process.

How to Configure a Product

The *Software Configuration Service (SCS)* facilitates the mainframe product configuration from the software inventory of the driving system to targeted z/OS operating systems.

You can use the SCS component of CA MSM to configure a CA Technologies product that you have already acquired, installed, and deployed.

You perform the following high-level tasks to configure your products using CA MSM:



1. From the Deployments tab, select a configurable deployment, select the associated product, and click Create Configuration to open the Configuration wizard.
2. Create the configuration by completing all the steps in the wizard:
   a. Define a configuration name and select a target system.
   b. Select configuration functions and options.
   c. Define system preferences.
   d. Create target settings.
   e. Select and edit resources.
3. Build the configuration. The last step of the Configuration wizard lets you build the configuration. If needed, you can edit the configuration and can build the configuration again.
4. Implement the configuration. The implementation process in CA MSM guides you and provides detailed instructions to start, stop, and manage the steps of the implementation process.

After the configuration process completes, the product is ready for you to use. Sometimes there are other steps to perform manually outside of CA MSM.

Note: You cannot use CA MSM to configure a product to a staging system.

Access CA MSM Using the Web-Based Interface

You access CA MSM using the web-based interface.

You need the URL of CA MSM from the CA MSM administrator.

Follow these steps:

1. Start your web browser, and enter the access URL.

   The login page appears.

   Note: If the Notice and Consent Banner appears, read and confirm the provided information.
2. Enter your z/OS login user name and password.

   The initial page appears. If you log in for the first time, you are prompted to define your account on the CA Support Online website.

   Note: For more information about the interface, click the online help link at the top right corner of the page.
3. Click New.

   You are prompted for the credentials to use on the CA Support Online website.

4. Specify the credentials, click OK, and then click Next.

   You are prompted to review your user settings.

   Note: These settings are available on the User Settings page.

5. Change the settings or keep the defaults, and then click Finish.

   A dialog opens, which shows the progress of the configuration task. You can click Show Results to view the details of the actions in a finished task.

Important! If your site uses proxies, review your proxy credentials on the User Settings, Software Acquisition page.

Chapter 4: Installing Your Product from Pax-Enhanced ESD

This section contains the following topics:

How to Install a Product Using Pax-Enhanced ESD

This section describes the Pax-Enhanced ESD process. We recommend that you read this overview and follow the entire procedure the first time you complete a Pax-Enhanced ESD installation. For experienced UNIX users, the *Pax-Enhanced ESD Quick Reference Guide* has sufficient information for subsequent installations.

Important! Downloading pax files for the SMP/E installation as part of the Pax-Enhanced ESD process requires write authority to the UNIX System Services (USS) directories that are used for the ESD process.

If you prefer not to involve all CA Technologies product installers with z/OS UNIX System Services, assign a group familiar with USS to perform Steps 1 through 4 and provide the list of the unpacked MVS data sets to the product installer. USS is not required for the actual SMP/E RECEIVE of the product or for any of the remaining installation steps.

To install files using Pax-Enhanced ESD, use the following process:

1. Allocate and mount the file system. This process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system that is dedicated to Pax-Enhanced ESD and create the directory in this file system. Ensure that all users who will be working with pax files have write authority to the directory.

2. Copy the product pax files into your USS directory. To download files, choose one of the following options:

   - Download a zip file from CA Support Online to your PC, unzip the file, and then upload the product pax files to your USS file system.
   - FTP the pax files from CA Support Online directly to your USS directory.

   Note: Perform Steps 3 through 6 for each pax file that you upload to your USS directory.

3. Create a product directory from the pax file. Set the current working directory to the directory containing the pax file, and create a directory in your USS directory by entering the following command:

   pax `-rvf` *pax-filename*

4. Use the SMP/E GIMUNZIP utility to create z/OS installation data sets. The file UNZIPJCL in the directory that the pax command created in Step 3 contains a sample JCL to GIMUNZIP the installation package. Edit and submit the UNZIPJCL JCL.

5. Receive the SMP/E package. Use the data sets that GIMUNZIP created in Step 4. Perform a standard SMP/E RECEIVE using the SMPPTFIN and SMPHOLD (if applicable) DASD data sets. Also, specify the high-level qualifier for the RELFILEs on the RFPREFIX parameter of the RECEIVE command.

6. Proceed with product installation. Consult product-specific documentation, including AREADME files and installation notes to complete the product installation.

7. (Optional) Clean up the USS directory. Delete the pax file, the directory that the pax command created, all of the files in it, and the SMP/E RELFILEs, SMPMCS, and HOLDDATA data sets.

More Information:

USS Environment Setup (see page 32)
Allocate and Mount a File System (see page 33)
Create a Product Directory from the Pax File (see page 41)
Copy Installation Files to z/OS Data Sets (see page 42)

How the Pax-Enhanced ESD Download Works

Important! To download pax files for the SMP/E installation as part of the Pax-Enhanced ESD process, you must have write authority to the UNIX System Services (USS) directories used for the ESD process and available USS file space before you start the procedures in this guide.

Use the following process to download files using Pax-Enhanced ESD:

1. Log in to https://support.ca.com/, and click Download Center.

   The CA Support Online web page appears.

2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and genlevel (if applicable), and click Go.

   The CA Product Download window appears.

3. Download an entire CA Technologies product software package or individual pax files to your PC or mainframe. If you download a zip file, you must unzip it before continuing.

   For both options, The ESD Product Download Window (see page 29) topic explains how the download interface works.

   Note: For traditional installation downloads, see the *Traditional ESD User Guide*. Go to https://support.ca.com/, log in, and click Download Center. A link to the guide appears under the Download Help heading.

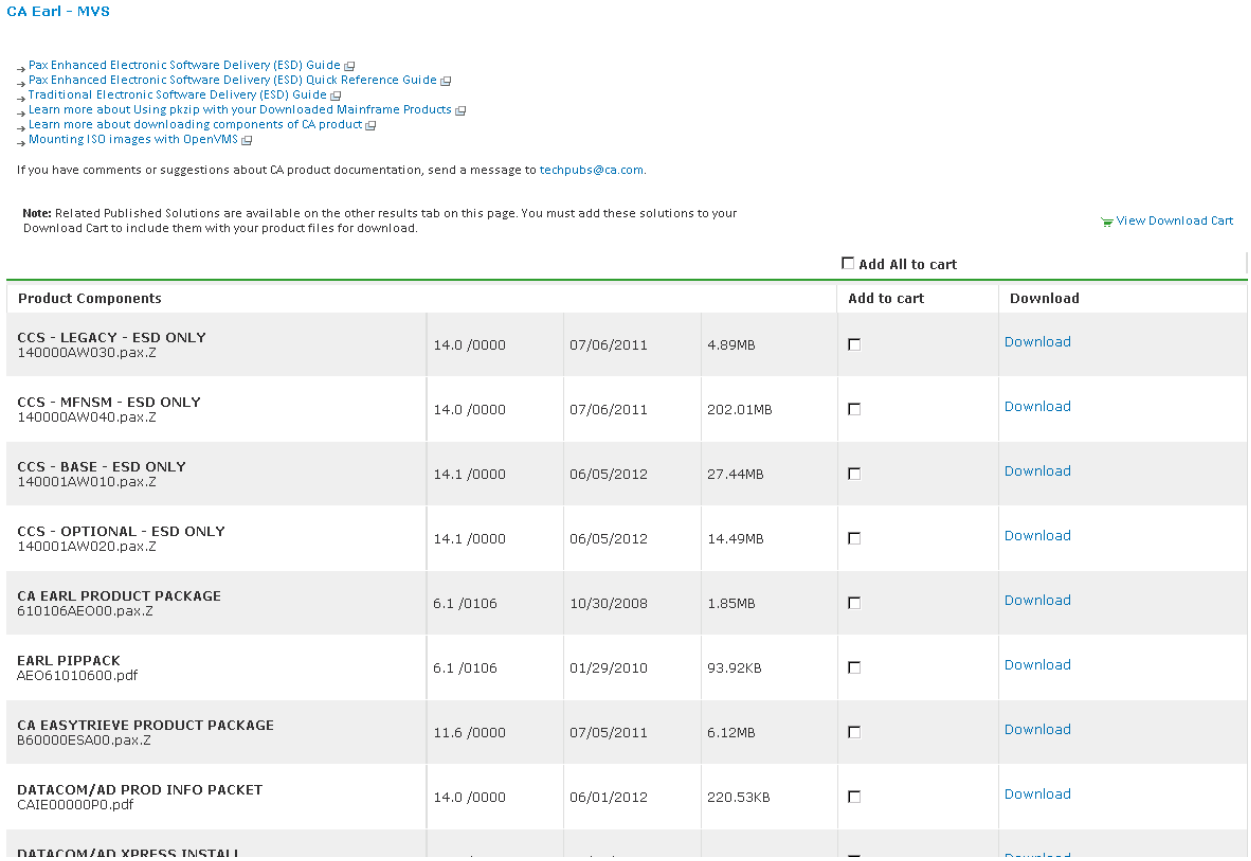
4. Perform the steps to install the product based on the product-specific steps.

   The product is installed on the mainframe.

ESD Product Download Window

You can download CA Technologies product ESD packages multiple ways. Your choices depend on the size of the individual files and the number of files that you want to download. You can download the complete product with all components, or you can select individual pax and documentation files for your product or component.

The following illustration shows sample product files. The illustration lists all components of the product. You can use the Download Cart by selecting one or more components that you need, or selecting the check box for Add All to cart. If you prefer to immediately download a component, click the Download link.



CA Earl - MVS

- Pax Enhanced Electronic Software Delivery (ESD) Guide
- Pax Enhanced Electronic Software Delivery (ESD) Quick Reference Guide
- Traditional Electronic Software Delivery (ESD) Guide
- Learn more about Using pkzip with your Downloaded Mainframe Products
- Learn more about downloading components of CA product
- Mounting ISO images with OpenVMS

If you have comments or suggestions about CA product documentation, send a message to techpubs@ca.com.

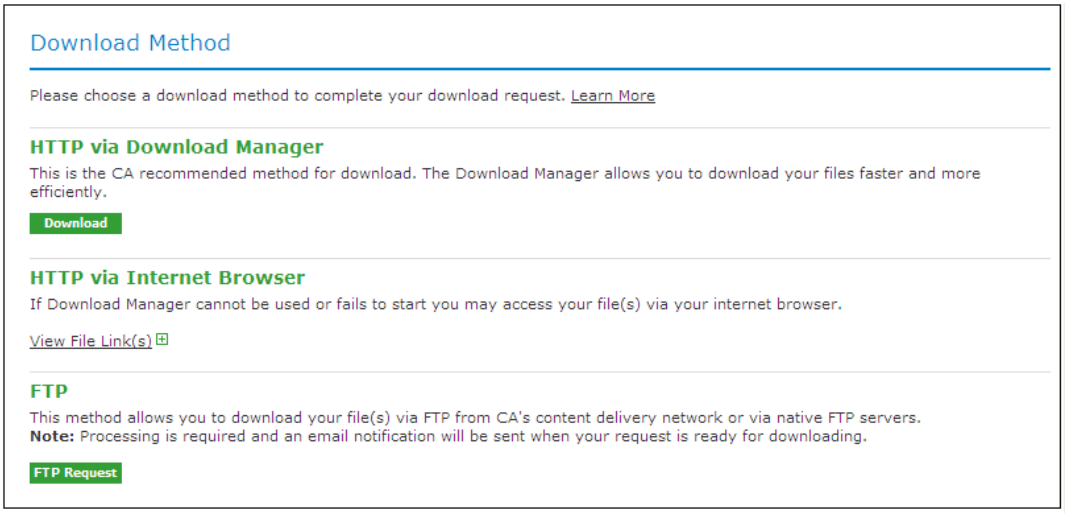
Note: Related Published Solutions are available on the other results tab on this page. You must add these solutions to your Download Cart to include them with your product files for download.

View Download Cart

Add All to cart

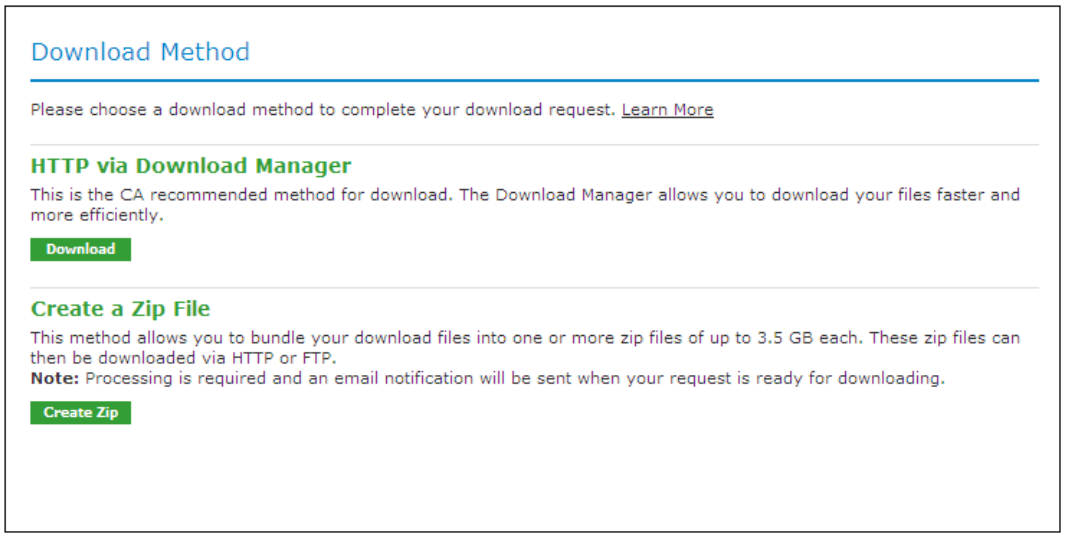
Product Components				Add to cart	Download
CCS - LEGACY - ESD ONLY 140000AW030.pax.Z	14.0 /0000	07/06/2011	4.89MB	☐	Download
CCS - MFNSM - ESD ONLY 140000AW040.pax.Z	14.0 /0000	07/06/2011	202.01MB	☐	Download
CCS - BASE - ESD ONLY 140001AW010.pax.Z	14.1 /0000	06/05/2012	27.44MB	☐	Download
CCS - OPTIONAL - ESD ONLY 140001AW020.pax.Z	14.1 /0000	06/05/2012	14.49MB	☐	Download
CA EARL PRODUCT PACKAGE 610106AE000.pax.Z	6.1 /0106	10/30/2008	1.85MB	☐	Download
EARL PIPPACK AE061010600.pdf	6.1 /0106	01/29/2010	93.92KB	☐	Download
CA EASYTRIEVE PRODUCT PACKAGE B60000ESA00.pax.Z	11.6 /0000	07/05/2011	6.12MB	☐	Download
DATACOM/AD PROD INFO PACKET CAIE00000P0.pdf	14.0 /0000	06/01/2012	220.53KB	☐	Download
DATACOM/AD XPRESS INSTALL				☐	Download

Clicking the link for an individual component takes you to the Download Method page.



Depending on the size and quantity of ordered product files, the Download Method screen could also have these options:

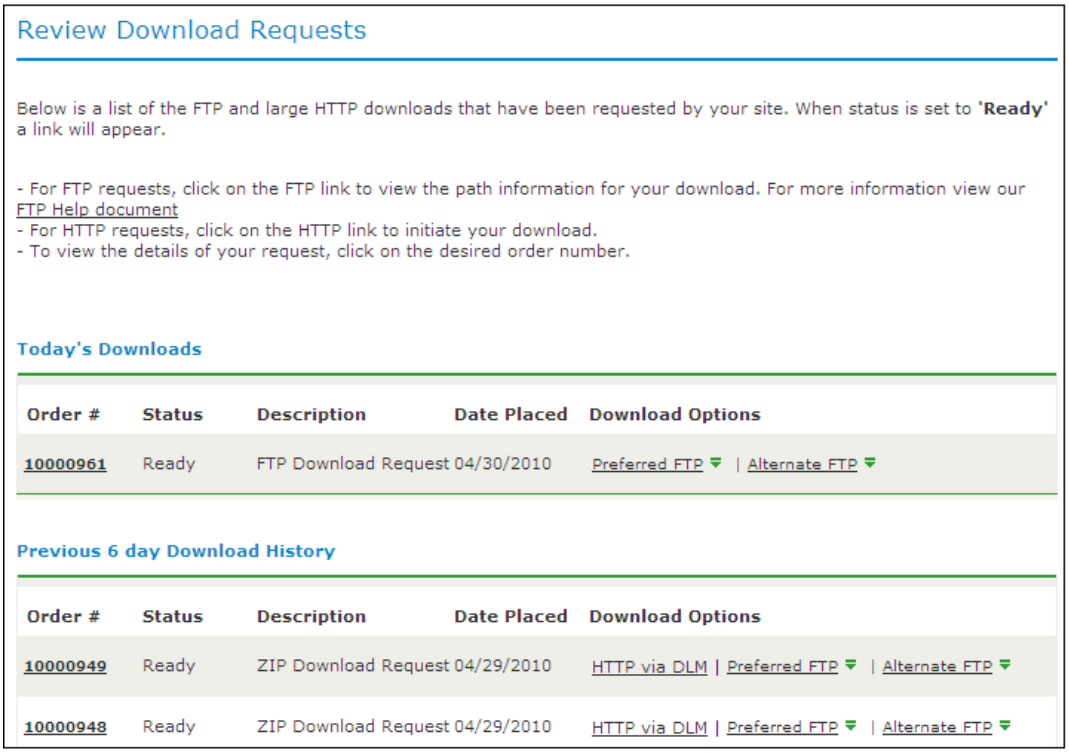
Note: For mainframe downloads using this HTTP method, click the Learn More link.



The HTTP method lets you start downloading immediately. The FTP method takes you to the Review Orders page that displays your order, first in a Pending status changing to Ready when your order has been processed.

Preferred FTP uses the new content delivery network (CDN). Alternate FTP uses the CA Technologies New York-based FTP servers.

The Create a Zip File option first creates the zip, and when ready, offers the options that the Zip Download Request examples show in the next illustration.



Review Download Requests

Below is a list of the FTP and large HTTP downloads that have been requested by your site. When status is set to **'Ready'** a link will appear.

- For FTP requests, click on the FTP link to view the path information for your download. For more information view our FTP Help document
- For HTTP requests, click on the HTTP link to initiate your download.
- To view the details of your request, click on the desired order number.

Today's Downloads

Order #	Status	Description	Date Placed	Download Options
10000961	Ready	FTP Download Request	04/30/2010	Preferred FTP | Alternate FTP

Previous 6 day Download History

Order #	Status	Description	Date Placed	Download Options
10000949	Ready	ZIP Download Request	04/29/2010	HTTP via DLM | Preferred FTP | Alternate FTP
10000948	Ready	ZIP Download Request	04/29/2010	HTTP via DLM | Preferred FTP | Alternate FTP

USS Environment Setup

You need a UNIX System Services (USS) directory and a file system with adequate space to perform the following tasks:

- Receive product pax files from CA Support Online.
- Perform utility functions to unpack the pax file into MVS data sets that you can use to complete the product installation.

We recommend that you allocate and mount a file system that is dedicated to Pax-Enhanced ESD. The amount of space that you need for the file system depends on the following variables:

- The size of the pax files that you intend to download.
- Whether you plan to keep the pax files after unpacking them. We do not recommend this practice.

We recommend that you use one directory for downloading and unpacking pax files. Reusing the same directory minimizes USS setup. You need to complete the USS setup only one time. You reuse the same directory for subsequent downloads. Alternatively, you can create a directory for each pax download.

Important! Downloading pax files for the SMP/E installation as part of the Pax-Enhanced ESD process requires write authority to the UNIX System Services (USS) directories that are used for the ESD process. The USS file system that is used for Pax-Enhanced ESD must have sufficient free space to hold the directory that the pax command created, and its contents. You need approximately 3.5 times the pax file size in free space to download the pax file and unpack its contents. For example, to download and unpack a 14 MB pax file, you need approximately 49 MB of free space in the file system hosting your ESD directory.

Allocate and Mount a File System

You can use the zSeries File System (zFS) or hierarchical file system (HFS) for ESD downloads.

This procedure describes how to perform the following tasks:

- Allocate a zFS or an HFS.
- Create a mount point in an existing maintenance USS directory of your choice.
- Mount the file system on the newly created mount point.

  Note: You must have either SUPERUSER authority, or the required SAF profile setting to allow you to issue the USS mount command for the file system.
- Optionally, permit write access to anyone in the same group as the person who created the directory.

  Important! USS commands are case-sensitive.

Follow these steps:

1. Allocate the file system by customizing one of the following samples to your site requirements:

   - On a zFS, use the following sample:

```
//DEFINE   EXEC PGM=IDCAMS
//SYSPRINT DD   SYSOUT=*
//SYSUDUMP DD   SYSOUT=*
//AMSDUMP  DD   SYSOUT=*
//SYSIN    DD *
  DEFINE CLUSTER ( +
  NAME(your_zFS_data_set_name) +
  STORAGECLASS(class) +
  LINEAR +
  CYL(primary secondary) +
  SHAREOPTIONS(3,3) +
  )
/*
//FORMAT   EXEC PGM=IOEAGFMT,REGION=0M,
// PARM=('-aggregate your_zFS_data_set_name -compat')
//SYSPRINT DD   SYSOUT=*
//SYSUDUMP DD   SYSOUT=*
//STDOUT   DD   SYSOUT=*
//STDERR   DD   SYSOUT=*
//CEEDUMP  DD   SYSOUT=*
//*
```

   - On an HFS, use the following sample:

```
//ALCHFS EXEC PGM=IEFBR14
//CAESD  DD   DSN=yourHFS_data_set_name,
//            DISP=(NEW,CATLG,DELETE),UNIT=3390,
//            DSNTYPE=HFS,SPACE=(CYL,(primary,secondary,1))
```

   The file system is allocated.

   Note: Ensure that the zFS or HFS data set name that you use conforms to your data set naming conventions for USS file systems. If the allocation of the file system data set fails, it is because of environmental settings not allowing for the allocation. On an HFS, try using the ISPF 3.2 Data Set Utility to allocate your HFS data set.

2. Create a mount point for the file system. This example shows how to create a /CA/CAESD directory in an existing directory, /u/maint. From the TSO OMVS shell, enter the following commands:

   ```
   cd /u/maint/
   mkdir CA
   cd CA
   mkdir CAESD
   ```

   Note: This document refers to this structure as *yourUSSESDdirectory*.

   The mount point is created.

3. Mount the file system by customizing one of the following samples to your site requirements:

   - On a zFS, use the following sample:

     ```
     MOUNT FILESYSTEM('your_zFS_data_set_name')
           MOUNTPOINT('yourUSSESDdirectory')
           TYPE(ZFS)  MODE(RDWR)
           PARM(AGGRGROW)
     ```

   - On an HFS, use the following sample:

     ```
     MOUNT FILESYSTEM('your_HFS_data_set_name')
           MOUNTPOINT('yourUSSESDdirectory')
           TYPE(HFS)  MODE(RDWR)
     ```

   The file system is mounted.

4. (Optional) Set security permissions for the directory. You can use the chmod command to let other users access the ESD directory and its files. For example, to allow write access to the ESD directory for other users in your USS group, from the TSO OMVS shell, enter the following command:

   ```
   chmod -R 775 /yourUSSESDdirectory/
   ```

   Write access is granted.

   Note: For more information about the chmod command, see the IBM *z/OS UNIX System Services User Guide* (SA22-7802).

Acquire the Product Pax Files

To begin the CA Technologies product installation procedure, copy the product pax file into the USS directory that you set up.

Important! Downloading pax files for the SMP/E installation as part of the Pax ESD process requires write authority to the UNIX System Services (USS) directories that are used for the Pax ESD process. Also, you must have available USS file space before you start the procedures in this guide.

Use one of the following methods:

- Download the product pax file from http://ca.com/support to your PC (see page 37), and then upload it to your USS file system.

  If you download a zip file, you must unzip it before uploading to your USS file system.
- Download the pax files from http://ca.com/support directly to your USS file system.
- Download the pax file from the product DVD to your PC, and then upload the pax files to your USS file system.

This section includes the following information:

- A sample batch job to download a product pax file from the CA Support Online FTP server directly to a USS directory on your z/OS system
- Sample commands to upload a pax file from your PC to a USS directory on your z/OS system

Important! The FTP procedures vary due to local firewall and other security settings. Consult your local network administrators to determine the appropriate FTP procedure to use at your site.

Ensure that sufficient free space is available in the USS file system that you are using to hold the product pax file. If you do not have sufficient free space, error messages similar to the following appear:

```
EZA1490I Error writing to data set
EZA2606W File I/O error 133
```

When the download finishes, the pax file size in your USS directory matches the value in the Size column for the corresponding pax file on the CA Technologies Products Download window.

More Information:

How the Pax-Enhanced ESD Download Works (see page 29)
ESD Product Download Window (see page 29)

Download Files to a PC Using Pax ESD

You can download product installation files from http://ca.com/support to your PC.

Follow these steps:

1. Log in to http://ca.com/support, and click Download Center.

   The Download Center web page appears.

2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and gen level (if applicable), and click Go.

   The CA Product Download window appears.

3. Download an entire CA Technologies product software package or individual pax files to your PC. If you download a zip file, you must unzip it before continuing.

   Note: For traditional installation downloads, see the *Traditional ESD User Guide*. For information about download methods, see the Download Methods and Locations article. Go to http://ca.com/support, log in, and click Download Center. Links to the guide and the article appear under the Download Help heading.

Download Using Batch JCL

Use this process to download a pax file from the CA Support Product Downloads window by running batch JCL on the mainframe. Use the sample JCL attached to the PDF file as CAtoMainframe.txt to perform the download.

Important! To simplify the Pax-Enhanced ESD process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the file to view the sample JCL.

Note: We recommend that you follow the preferred method as described on CA Support Online. This procedure is our preferred download method; however, we do include the procedure to download to the mainframe through a PC in the next section.

Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCP/IP profile data set for your system. Consult your local network administrators, if necessary.

   The job points to your profile.

3. Replace *YourEmailAddress* with your email address.

   The job points to your email address.

4. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

   The job points to your USS directory.

5. Locate the product component to download on the CA Support Product Download window.

   You have identified the product component to download.

6. Click Download for the applicable file.

   Note: For multiple downloads, add files to a cart.

   The Download Method window opens.

7. Click FTP Request.

   The Review Download Requests window displays any files that you have requested to download.

   Note: We send you an email when the file is ready to download or a link appears in this window when the file is available.

8. Select one of the following methods:

   Preferred FTP

   Uses CA Technologies worldwide content delivery network (CDN). If you cannot download using this method, review the security restrictions for servers that company employees can download from that are outside your corporate network.

   Host Name: ftp://ftpdownloads.ca.com

   Alternate FTP

   Uses the original download servers that are based on Long Island, New York.

   Host Name: ftp://scftpd.ca.com for product files and download cart files and ftp://ftp.ca.com for individual solution files.

   Both methods display the host, user name, password, and FTP location, which you then can copy into the sample JCL.

   Note: The following links provide details regarding FTP: the FTP Help document link in the Review Download Requests window and the Learn More link available in the Download Methods window.

9. Submit the job.

   Important! If your FTP commands are incorrect, it is possible for this job to fail and still return a zero condition code. Read the messages in the job DDNAME SYSPRINT to verify the FTP succeeded.

   After you run the JCL job, the pax file resides in the mainframe USS directory that you supplied.

Example: CAtoMainframe.txt, JCL

The following text appears in the attached CAtoMainframe.txt JCL file:

```
//GETPAX   JOB (ACCOUNTNO),'FTP GET ESD PACKAGE',
//          MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*********************************************************************
//* This sample job can be used to download a pax file directly from  *
//* CA Support Online to a USS directory on your z/OS system.         *
//*                                                                   *
//* When editing the JCL ensure that you do not have sequence numbers *
//* turned on.                                                        *
//*                                                                   *
//* This job must be customized as follows:                           *
//* 1. Supply a valid JOB statement.                                  *
//* 2. The SYSTCPD and SYSFTPD JCL DD statements in this JCL may be   *
//*    optional at your site. Remove the statements that are not      *
//*    required. For the required statements, update the data set     *
//*    names with the correct site-specific data set names.           *
//* 3. Replace "Host" based on the type of download method.           *
//* 4. Replace "YourEmailAddress" with your email address.            *
//* 5. Replace "yourUSSESDdirectory" with the name of the USS         *
//*    directory used on your system for ESD downloads.               *
//* 6. Replace "FTP Location" with the complete path                  *
//*    and name of the pax file obtained from the FTP location        *
//*    of the product download page.                                  *
//*********************************************************************
//GETPAX   EXEC PGM=FTP,PARM='(EXIT',REGION=0M
//SYSTCPD  DD   DSN=yourTCPIP.PROFILE.dataset,DISP=SHR
//SYSFTPD  DD   DSN=yourFTP.DATA.dataset,DISP=SHR
//SYSPRINT DD   SYSOUT=*
//OUTPUT   DD   SYSOUT=*
//INPUT    DD   *
Host
anonymous YourEmailAddress
lcd yourUSSESDdirectory
binary
get FTP_location
quit
```

Download Files to Mainframe through a PC

If you download pax or zip files from CA Support Online to your PC, use this procedure to upload the pax file from your PC to your z/OS USS directory.

Follow these steps:

1. Follow the procedures in How the Pax-Enhanced ESD Download Works (see page 10) to download the product pax or zip file to your PC. If you download a zip file, first unzip the file to use the product pax files.

   The pax or zip file resides on your PC.

2. Open a Windows command prompt.

   The command prompt appears.

3. Customize and enter the FTP commands with the following changes:

   a. Replace *mainframe* with the z/OS system IP address or DNS name.

   b. Replace *userid* with your z/OS user ID.

   c. Replace *password* with your z/OS password.

   d. Replace *C:\PC\folder\for\thePAXfile* with the location of the pax file on your PC.

   e. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

   f. Replace *paxfile.pax.Z* with the name of the pax file to upload.

   The pax file is transferred to the mainframe.

Example: FTP Commands

This list is a sample of FTP commands to upload the pax file from your PC to your USS Pax-Enhanced ESD directory:

```
ftp mainframe
userid
password
bin
lcd C:\PC\folder\for\thePAXfile
cd /yourUSSESDdirectory/
put paxfile.pax.Z
quit
exit
```

Create a Product Directory from the Pax File

Use the sample job attached to the PDF file as Unpackage.txt to extract the product pax file into a product installation directory.

Important! To simplify the Pax-Enhanced ESD process, the PDF version of this guide includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the file to view the sample JCL.

Follow these steps:

1. Supply a valid JOB statement.
2. Replace *yourUSSESDdirectory* with the name of the USS directory that you use for ESD downloads.

   The job points to your specific directory.
3. Replace *paxfile.pax.Z* with the name of the pax file.

   The job points to your specific pax file.
4. Submit the job.

   The job runs and creates the product directory.

Note: If the PARM= statement exceeds 71 characters, uncomment and use the second form of UNPAXDIR instead. This sample job uses an X in column 72 to continue the PARM= parameters to a second line.

Sample Job to Execute the Pax Command (Unpackage.txt)

The following text appears in the attached Unpackage.txt JCL file:

```
//ESDUNPAX JOB (ACCOUNTNO),'UNPAX ESD PACKAGE ',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*********************************************************************
//* This sample job can be used to invoke the pax command to create   *
//* the product-specific installation directory.                      *
//*                                                                   *
//* This job must be customized as follows:                           *
//* 1. Supply a valid JOB statement.                                  *
//* 2. Replace "yourUSSESDdirectory" with the name of the USS         *
//*    directory used on your system for ESD downloads.               *
//* 3. Replace "paxfile.pax.Z" with the name of the pax file.         *
//* NOTE: If you continue the PARM= statement on a second line, make  *
//*       sure the 'X' continuation character is in column 72.        *
//*********************************************************************
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSESDdirectory/; pax -rvf paxfile.pax.Z'
//*UNPAXDIR EXEC PGM=BPXBATCH,
//* PARM='sh cd /yourUSSESDdirectory/; pax                            X
//*            -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

Copy Installation Files to z/OS Data Sets

Use this procedure to invoke the SMP/E GIMUNZIP utility to create MVS data sets from the files in the product-specific directory.

Follow these steps:

1. Locate and read the product readme file or installation notes, if applicable, which resides in the product-specific directory that the pax command created. This file contains the product-specific details that you require to complete the installation procedure.

   You have identified the product-specific installation details.

2. Use ISPF EDIT or TSO ISHELL to edit the UNZIPJCL sample job. You can perform this step in one of the following ways:

   - Use ISPF EDIT. Specify the full path name of the UNZIPJCL file.
   - Use TSO ISHELL. Navigate to the UNZIPJCL file and use the E line command to edit the file.

   The job is edited.

3. Change the SMPDIR DD PATH to the product-specific directory created by the pax command.

   Your view is of the product-specific directory.

4. If ICSF is not active, perform the following steps:

   a. Change the SMPJHOME DD PATH to your Java runtime directory. This directory varies from system to system.

      Note: The default Java location is the following:

      `/usr/lpp/java/Java_version`

   b. Perform one of the following steps:

      - Change the SMPCPATH DD PATH to your SMP/E Java application classes directory, typically /usr/lpp/smp/classes/.
      - Change HASH=YES to HASH=NO on the GIMUNZIP parameter.

   One of the following occurs: ICSF is active, or you are using Java.

5. Change all occurrences of y*ourHLQ* to the high-level qualifier (HLQ) for z/OS data sets that the installation process uses. We suggest that you use a unique HLQ for each expanded pax file to identify uniquely the package. Do *not* use the same value for y*ourHLQ* as you use for the SMP/E RELFILEs.

   All occurrences of y*ourHLQ* are set to your high-level qualifier for z/OS data sets.

6. Submit the UNZIPJCL job.

   The UNZIPJCL job completes with a zero return code. Messages GIM69158I and GIM48101I in the output and IKJ56228I in the JES log are acceptable.

   GIMUNZIP creates z/OS data sets with the high-level qualifier that you specified in the UNZIPJCL job. You use these data sets to perform the product installation. The pax file and product-specific directory are no longer needed.

   Note: For more information, see the IBM *SMP/E for z/OS Reference (SA22-7772)*.

Customize the Installation JCL

Customize the installation JCL in the SAMPJCL data set to allocate and load the required data sets.

To customize the installation JCL

1. Edit and submit the DEFSMPE member of the SAMPJCL data set.

   This job defines and initializes the SMP/E control data sets.

2. Edit and submit the JCL in the INSTTPXD member of the SAMPJCL data set. Comments in the JCL specify what information you must supply or modify. The job executes successfully with a condition code of 0.

Clean Up the USS Directory

Important! This procedure is optional. Do not use this procedure until you complete the entire installation process.

To free file system disk space for subsequent downloads after downloading and processing the pax files for your CA Technologies product, we recommend removing the files from your USS directory and deleting unnecessary MVS data sets. You can delete the following items:

- Pax file
- Product-specific directory that the pax command created and all of the files in it
- SMP/E RELFILEs, SMPMCS, and HOLDDATA MVS data sets

  These data sets have the HLQ that you assigned in the UNZIPJCL job.

Note: Retain non-SMP/E installation data sets such as *yourHLQ*.INSTALL.NOTES for future reference.

Follow these steps:

1. Navigate to your Pax-Enhanced ESD USS directory.

   Your view is of the applicable USS directory.

2. Delete the pax file by entering the following command:

   `rm paxfile`

   paxfile

   Specifies the name of the CA Technologies pax file that you downloaded.

   The pax file is deleted.

3. Delete the product-specific directory by entering the following command:

   `rm -r` *`product-specific_directory`*

   product-specific_directory

   Specifies the product-specific directory that the pax command created.

   The product-specific directory is deleted.

Note: You can also use TSO ISHELL to navigate to the pax file and product-specific directory, and delete them using the D line command.

Chapter 5: Configuring Your Product

This section describes the minimum configuration tasks needed before CA TPX can be started, customized, and used in your environment.

This section contains the following topics:

Calculate VSAM Storage

To calculate the number of VSAM storage records needed for the ADMIN2 file use:

`VSAM storage records = profs + profsessions + users + usersessions`

where:

profs

Indicates number of profiles

profsessions

Indicates total *number* of sessions in all profiles

users

Indicates number of *users*

usersessions

Indicates total *number* of sessions for all users

Edit and submit the JCL in the DEFVSAM member of the CB0VJCL data set. Comments in the JCL specify the information that you must supply or modify. The job executes successfully with a condition code of 0.

Define APPL Statements

This task adds APPL statements to your SYS1.VTAMLST data set. The APPL statements define the following logical units to VTAM:

- CA TPX application
- Virtual terminals
- Virtual printers

The definitions allow the product to establish application sessions with virtual terminals and perform pass-through printing. The definitions are contained in the APTPX member of the CB0VSRC data set.

For a description of the APPL statements see the appendix APPL Statements (see page 79).

For details on virtual terminals and passthrough printing, see the *Administration Guide.*

To copy the APPL statements to your SYS1.VTAMLST data set you can:

- Edit and submit the TPXAPPL member of the CB0VJCL data set.
- Copy the APTPX member of the CB0VSRC data set using the ISPF copy facility.

Using TPXAPPL

If you use the TPXAPPL member:

1. Specify the following information in the member:
   - An appropriate job card.
   - A name for the member when it is copied to SYS1.VTAMLST. You can give the member a name other than APTPX, as long as it is specified on the TPXAPPL parameter in the startup procedure.
   - Any required changes to the SYSIN data.

   The member containing the APPL statements relating to the product must include these comment lines:

```
*TPX,PRIMARY
*TPX,REBIND
*TPX,SHARE
*TPX,GROUP
*TPX,UNIQUE
*TPX,APPLPPS
*TPX,USERPPS
```

Each comment line must appear just before its corresponding APPL statements.

Important! If cross-domain resources need to be defined at your site, change the condition code of the CDSC parameter on the PROC statement to 4.

2. Submit the TPXAPPL job.

   The job executes successfully with a condition code of 0.

Note: When going production, it may be appropriate to use VTAM model statements instead of those defined in the TPXAPPL member. For more information, see the *Batch Administration Guide*.

Copy the Logmode Tables

Logmode tables define virtual terminals to the product. When a 3270-type terminal user requests a session, CA TPX selects the appropriate entry from the logmode table to define a virtual terminal session that is suitable for the terminal of that user.

The TPX.CB0VSRC data set contains five logmode tables that you must copy to your SYS1.VTAMLIB data set.

The basic table, TPXLGMOD, contains entries that define session parameters for almost any 3270 terminal model. These entries are duplicated in tables TPXLGMD2 through TPXLGMD5.

An additional entry is added to these tables to allow the incorporation of Dynamic Logmodes for ANY terminal model. The following example shows the additional entry added to the PSERVIC parameter:

```
PSERVIC=X'028000000000000000000300'
```

The multiple tables can be customized for applications that require an entry with a particular name, regardless of the terminal model. The logmode tables include an entry to allow LU1 terminal support.

For additional information about using the logmode tables and creating entries for applications with special requirements, see the *Programming Guide*.

To copy the tables

1. Submit the JCL in the LOGMODE member of the CB0VJCL data set on each system where CA TPX will run.
2. If your site has user-defined logmode tables in a separate library, change the data set name in the LOGMODE job to refer to this library.

Copy the Startup Procedure

If you are using CA-L-Serv to manage all or some of the VSAM files, you must copy the startup procedure that you modified as described in the appendix VSAM File Sharing With CA-L-Serv (see page 71). Do not submit TPXPROC.

To copy the startup procedure to your PROCLIB

1. If you have deviated from the naming conventions used in this guide, modify the JCL in TPXPROC as necessary:
   - Change the PREFIX parameter to match the prefix specified for the data sets when they were loaded.
   - Make sure the name on the PROC statement is unique for each component installed at your site.
   - Make sure the APPL parameter matches the name of the SYS1.VTAMLST member created when you defined APPL statements.
2. Make sure that the JCL:
   - Allows a region size of at least 4 MB to start the product. You may need to adjust this value for production.
   - Specifies the CB0VPENU panel library in addition to any other panel libraries.
3. To write the log to a data set other than SYSOUT, specify a LOG data set with the specifications:
   - LRECL=131
   - RECFM=FBA

   Note: Do not set the log destination and class parameters in the System Options Table (SMRT) if logging is done to a non-SYSOUT data set.
4. Submit the JCL for the TPXPROC job. The job executes with a condition code of 0.

Authorize the Load Library

CA TPX must run from an APF-authorized library if you intend to use the following features:

- VTAM Authorized Path Facility
- VSAM file sharing
- VTAM Generic Resource Option
- TCPaccess Telnet Server interface

To authorize the CA TPX load library and any user load library, you must add them to SYS1.PARMLIB using one of the following methods:

- The older Authorized Program Facility List (IEAAPFxx) method
- The newer APF portion of Authorized Program List, Exits, LNKLST Sets and LPA (PROGxx) method

Note: For detailed information, see the IBM *z/OS MVS Initialization and Tuning Reference* for your release of the operating system.

Authorize the Load Library Using IEAAPFxx Method

To authorize the Load Library using the IEAAPFxx method

1. Add the data set name and volume of the load library to SYS1.PARMLIB(IEAAPFxx).
2. Add the data set name and volume of the CA TPX USERLIB to SYS1.PARMLIB(IEAAPFxx).
3. If you have a separate load library that contains your exit routines, add an entry in IEAAPFxx for that library as well.

Note: The xx in IEAAPFxx is the suffix of the authorization list specified in IEASYSxx.

Authorize the Load Library Using PROGxx Method

To authorize the Load Library using the PROGxx method

1. Add the data set name and volume of the load library using the ADD APF statement to SYS1.PARMLIB(PROGxx).
2. Add the data set name and volume of any CA TPX user library using the ADD APF statement to SYS1.PARMLIB(PROGxx).
3. If you have a separate load library that contains your exit routines, add an entry in PROGxx for that library as well.

Note: The xx in PROGxx is the suffix of the authorized program list specified in IEASYSxx.

Install Other Language Panels

Besides the default English panels, TPX also supports panels in the following languages:

- Belgium French
- Brazilian Portuguese
- Danish

- Dutch
- Finnish
- French
- German
- Italian
- Japanese
- Norwegian
- Swiss French
- Swiss German
- Spanish
- Swedish
- Upper Case English

To add one or more panel libraries

- Installing from files produced by the ESD process

  Edit and submit the JCL in the INSTPNLD member of the CB0VJCL data set.

  Comments in the JCL specify what information you must supply or modify. The job executes successfully with a condition code of 0.

Chapter 6: Starting Your Product

This chapter describes how to start and log on to CA TPX for the first time.

Note: If your site is using CA-L-Serv to manage the VSAM files, you must start CA-L-Serv before you start CA TPX. See the CA Common Services for z/OS documentation.

This section contains the following topics:

Issue Console Commands

To start the product, issue the console commands:

```
V NET,ACT,ID=APTPX
S TPX
```

You receive startup messages followed by a message that the product is accepting logons.

Note: If your site is using CA-L-Serv to manage the ADMIN1 or ADMIN2 files, and CA-L-Serv is unavailable, the product abends with a U001 abend. If your site is using CA-L-Serv for the NOTES, MAIL, or VIEW files only, the product will start without those files and will wait for CA-L-Serv to become available.

Log On a Terminal to CA TPX

When you have started the product, establish a connection between it and your terminal by issuing the command:

```
LOGON APPLID(TPX)
```

Note: The command you issue can have a different format if the VTAM system programmer at your site has altered the distributed Unformatted System Services (USS).

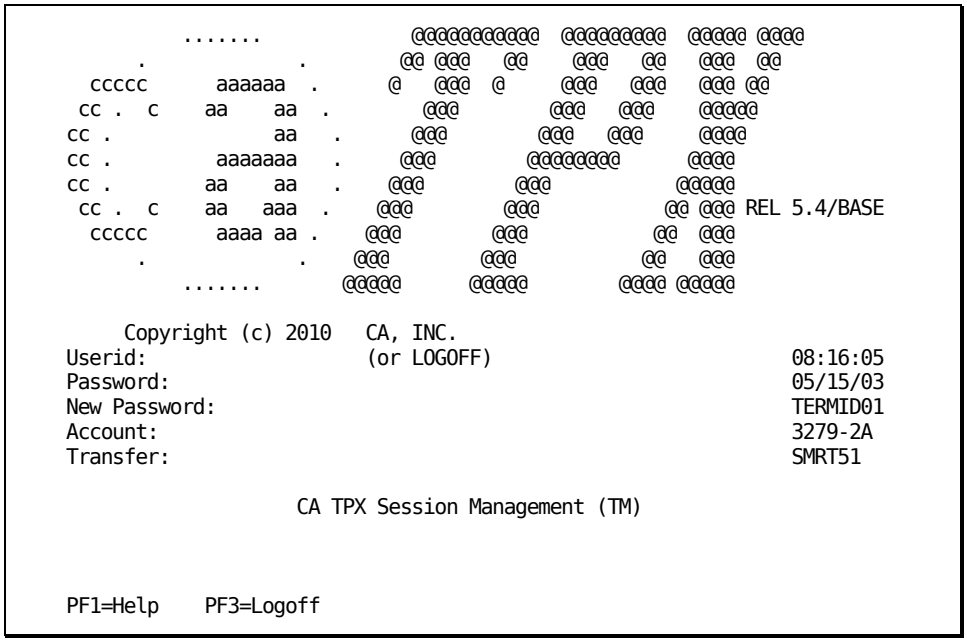
The USS component of VTAM converts this command to a request to initiate the application. VTAM honors this request as long as you have done both of the following:

- Defined a primary logical unit (PLU) named TPX on an APPL statement in the SYS1.VTAMLST data set.
- Activated the product by issuing the console commands specified in the section Starting CA TPX.

If using the TCPaccess Telnet Server interface, the 3270 emulator settings must specify the host IP address and port assigned to CA TPX in the Server. When the IP session is established, the user will see the TPX logon screen.

The Default Logo Panel

In response to the logon command, the default Logo panel appears, shown here:



The statements defining this screen initially reside in the T*ln*0003 member of the language panel data set, where *ln* specifies a language code. For a list of available languages, see Install Other Language Panels (see page 51).

Sign On to CA TPX

After the Logo panel appears, you can sign on to the product. Enter the pre-existing administrative user ID, TPXADMIN, which has unlimited authority.

Note: If CA TPX is used exclusively to administer CA STX, use the STXADMIN user ID.

If your site has not loaded the administration files, you need to add the TPXADMIN user ID with the Batch facility. JCL in the TPXADMIN member of the TPX.CB0VSRC will add this ID to your administration files.

To sign on to an LU1 terminal, enter the user ID and password, separated by a slash (/).

After the product accepts and processes your user ID, the Menu panel appears as shown in the following sample panel:

```
                        TPX MENU FOR      TPXADMIN          Panelid  - TEN0041
                                                            Terminal - ABDC1234
Cmdkey=PF12/24    Jump=PF20      Menu=PF19                  Model    - 3279-2
Print=NONE        Cmdchar=/                                 System   - TPXPROD

   Sessid      Sesskey       Session Description            Status

 _ TSO         PF  5         TSO on System1
 _ IMS         PF  6         IMS Production
 _ CICS        PF  7         CICS Test System
 _ TPXADMIN    PF  8         TPX Administration
 _ TPXMAIL     PF  9         TPX Mail System
 _ TPXNOTES    PF  10        TPX Notepad
 _ WINDOWS     PF  2         TPX Windows


Command ===>
PF1=Help  PF7/19=Up  PF8/20=Down  PF10/22=Left  PF11/23=Right  H =Cmd Help
```

After signing on, you can establish virtual terminal sessions with any application in your VTAM network except those that require the terminal to be predefined.

For instructions on using the menu, see the *User Guide*.

Stop CA TPX

To stop CA TPX, issue the console command:

```
P TPX
```

For information on stopping CA-L-Serv, see the CA Common Services for z/OS documentation.

Chapter 7: Post-Installation Tasks

This chapter gives a brief explanation of customization tasks and describes where you can find detailed information.

This section contains the following topics:

Use Authorized Path Facility

With the load modules in an authorized library, the product can run as a non-swappable application and use the VTAM Authorized Path Facility (APF) and write SMF records. The APF facility saves 20 to 30 percent of your CPU overhead. The APF facility is required for VTAM generic resource support.

To use VTAM Authorized Path Facility

1. Specify Y in the VTAM Authorized Path Facility field of the Performance Parameters panel.

   For information about changing the performance parameters, see the *Administration Guide*.

2. Specify YES on the SRBEXIT parameter of each APPL statement in your major node.

Define the Coupling Facility Structure

When using CA TPX to operate as a VTAM generic resource, you need to define the Coupling Facility structure.

Note: To use this feature, CA TPX must run from an APF-authorized library.

To define the Coupling Facility structure

1. Open member CFSTRUCT in the CB0VJCL data set.
2. Define the name of your structure and its size. Note the structure name consists of two parts:
   - An eight-byte prefix, which cannot contain blanks.
   - The generic resource name used for all instances of the product. You may need more than one generic resource name.

   Note:

   Each generic resource name requires its own structure.

   For details on determining the structure storage requirements, see the *Programming Guide.*
3. Update the z/OS policy data set to reflect the definition of the structure.
4. Once CA TPX is installed and running, update the generic resource parameters using the System Options Table Menu and then recycle CA TPX. For more information, see the *Administration Guide*.

Enable the TCPaccess Telnet Server Interface

The TCPaccess Telnet Server interface provides native IP support.

Note: To use this feature, CA TPX must run from an APF-authorized library.

Note the following:

- The interface is mutually exclusive with the VTAM Generic Resource Option.
- When using the interface, CA TPX provides TN3270 Server services in coordination with TCPaccess; therefore, the following CA TPX features will not be available when the interface is used:
  - Affinity feature
  - Pass Mode
  - The Pass Option on application definitions

Customize the JCL

Review the samples of TPXPROC and the CA TPX startup job stream you are using.

The ddname of VTAMLIB must point to the loadlib where the Modetab used to define terminal characteristics resides. This library is usually SYS1.VTAMLIB and is coded as such in the sample; correct it as necessary. The MODETAB parameter on the startup procedure identifies the mode table CA TPX is to use for terminal characteristics. If the MODETAB parameter is omitted, the default value of ISTINCLM is used.

Activate the Feature

After CA TPX is installed and running, you must set an option in the System Options Table (SMRT) to activate the interface.

Under System Features in the SMRT, specify Y in the Activate TCPaccess Telnet Interface field. For information about setting parameters in the SMRT, see the *Administration Guide.*

Recycle CA TPX to effect the change.

For information about activating the CA TPX interface on the TCPaccess Telnet Server, see the *CA TCPaccess Telnet Server Customization Guide*, the appendix "Native IP Interface."

Define Administrators

CA TPX allows you to distribute the responsibility for administration among several types of administrators. The capabilities of each administrator are assigned by a Master Administrator. To perform administration, you must define these administrators in an online administration session.

For instructions for defining administrators and running an online administration session, see the *Administration Guide*.

Define System Options and Applications

System administration gives you control over the operating environment. You must define the components for the VTAM network at your site and provide the product with information about applications, physical terminals, and printers. You also specify default system, application, and user characteristics.

For procedures relating to system administration, see the *Administration Guide*.

For a list of applications that require special customization tasks and the related procedures for these applications, see the *Programming Guide*.

Define Operator Capabilities

You can define the capabilities of operators by creating and maintaining operator command classes.

For instructions on specifying operator capabilities, see the *Administration Guide*.

To learn about the tasks operators perform in an operator session, see the *Operator Guide*.

For information about messages, see the *Message Reference Guide*.

Define Users

You can define users by using online or batch administration.

For information about performing user administration using the online facility, see the *Administration Guide*.

For information about performing user administration using the batch facility, see the *Batch Administration Guide*.

How you define user characteristics depends on what type of user you are defining, static or dynamic.

Static Users

Static users are defined in user administration and recorded in the administration databases. The characteristics of a static user are determined during signon by values in the System Options Tables, Application Definition Tables, and user and profile records.

Note: For a description of how user characteristics are determined, see the *Administration Guide*.

Dynamic Users

Dynamic users are not recorded in the administration databases. The characteristics of dynamic users are determined by profiles assigned in the signon exit. User validation and profile selection can be determined at signon through interaction with an external security package. The default signon exit provides for this method of dynamic user management and almost eliminates the need for ongoing user maintenance in CA TPX.

Options in the System Options Table (SMRT) determine if CA TPX accepts dynamic users. For information about the SMRT, see the *Administration Guide*.

The product also allows saved dynamic users.

Dynamic users cannot be administered because no record of them is kept in the ADMIN2 database. A user is either static or dynamic, and cannot be static for one component and dynamic for the other.

Allow Dynamic Users

To allow dynamic users, specify Y in the Dynamic Users Allowed field of the System Options Table (SMRT). The signon exit determines the profiles that are assigned to dynamic users.

Note: For more information on the signon exit, see the *Programming Guide*.

Convert Dynamic Users to Static Users

You can convert dynamic users to static users. This conversion can be set to take place automatically when the dynamic users sign on to the product. This procedure can be used to add new static users when they sign on, without having to administer them individually with online or batch administration.

Convert Users to a Different Type

To convert dynamic users into static users with signon privileges

1. Set the following fields to Y in the System Options Table (SMRT):
   - Allow Dynamic Users
   - Save Dynamic Users
   - Optional Parameter 18
2. Have users at your site sign on to the product at their convenience. The users will be assigned user characteristics as if they were dynamic users and these values will become their characteristics as static users. As soon as they sign on, they become static users with signon privileges.

A user administrator can also use the Static User field in User Options to determine whether a user is static or dynamic. This applies only to saved dynamic users.

Important! Remember to set Optional Parameter 18 to N after your users have become static to prevent spurious user IDs from being stored in your administration file.

Saved Dynamic Users

Saved dynamic users have the following features:

- Like dynamic users, the profiles specified in the signon exit (and optionally determined through interaction with external security) determine their session options.
- Unlike dynamic users, their user options are saved in the ADMIN2 database and can be modified by a user administrator or through self-maintenance.
- When profiles for a user for which CA TPX maintains user customization are no longer authorized by the signon exit or external security, those customizations are deleted at signon time. User IDs must be deleted manually.

Allowing saved dynamic users at your site gives you the convenience of dynamic users with the additional benefit of being able to administer them.

To allow saved dynamic users at your site, set the Save Dynamic Users option to Y in the System Options Table (SMRT). With this option turned on, all users who sign on dynamically become saved dynamic users.

The Static User field in the User Options panel can be set by a user administrator to change a saved dynamic user into a static user (or conversely). If a saved dynamic user becomes a static user, the profiles that were assigned when the user signed on are recorded in the user record and will be the profiles of the user every time the user signs on. The profiles of the user are no longer determined by the signon exit.

Write ACL/E Program

The product provides an automated conversation language (ACL/E) to help you automate and simplify information exchanges between users and their applications. The ACL/E program provides input in place of the user during user-application interactions.

For information on developing and using ACL/E programs, see the *ACL/E Programming Guide*.

For information on user interaction with applications through the product, see the *User Guide*.

Set Up VSAM Sharing

You can set up the product to allow the VSAM administration data sets to be shared. This allows you to run multiple regions and run batch administration while running the product online.

More information:

VSAM File Sharing Without CA-L-Serv (see page 69)

Implement a Signon and Signoff Exit

You can either use the default signon and signoff user exit, TPXUSNSF, which is distributed in the TPX.CB0VSRC, or use a signon and signoff exit of your own. If you do not specify a signon and signoff exit, the product uses the default exit.

Note: For information about the signon and signoff user exit, see the *Programming Guide*.

MAIL and VIEW Files

The installation procedure included allocation for the MAIL and VIEW files, which are VSAM files used by CA TPX for the Mail and View facilities.

If your site is not authorized to use the View facility or the MAIL facility, you do not need these files and can delete them. However, the VIEW file includes sample session recordings for use with the Record/Playback feature of the View facility. These sample recordings can be played back even if you are not authorized for View. The samples contain examples demonstrating the use of some features.

Chapter 8: Migration Information

This chapter describes considerations when migrating from a previous release of CA TPX.

This section contains the following topics:

Migration from Releases Prior to r4

r5.3 can share files with r4 and above. Administration should be performed from r5.3. Any settings in r5.3 that are not recognized by older releases are ignored and the associated functionality is not present when executing the older release.

Coupling Facility System Managed Rebuild

If r5.3 and any release prior to r5.2 are connected to the same Coupling Facility structure, a request to rebuild or alter the structure will be rejected by the operating system. To exploit the system managed rebuilding or altering of the Coupling Facility structure, all instances must be running either r5.2 or r5.3.

Migration Checklist

Use this checklist when migrating to a new release of CA TPX:

- Use the file allocations from the new CA TPX as delivered.
- Make a backup of your old CA TPX VSAM files.
- Copy the CA TPX VSAM file backups into the new allocated VSAM files.
- Verify that LOADLIB is APF authorized.
- Run RESET INTEGRITY (refer to CB0VSRC library, member BATCHINI).
- Migrate any custom ACL/E programs to the new ACL/E library.
- Migrate any custom PANEL libraries to the new PANEL library.
- Reassemble all custom user exits against the new libraries.
- Modify the new CA TPX startup procedure to refer to tables from migrated files (for example, SMRT, ACT, and so on).

- Review new SMRT parameters:
  1. Take screen prints of each SMRT panel in your existing release.
  2. Create a new SMRT in the new release and take screen prints of these.
  3. Compare both the SMRTs to identify new fields and their defaults.

     If you apply no changes to the SMRT in the new release, the defaults will be in effect for any new fields introduced since your existing release.

Note: As of r4, VSAM files are upwardly compatible and do not require conversion.

Chapter 9: Frequently Asked Questions

The following questions and answers will help you get started using CA TPX and its various features.

This section contains the following topics:

FAQs

Q: What is the recommended dispatch level?

A: Set the dispatch level to below VTAM and the TN3270 Server, but higher than applications that CA TPX communicates with (CICS, IMS, TSO, and so on), regardless of whether CA TPX is defined as a generic resource.

Q: Does a new service pack require that I reinstall the software?

A: No.

Q: What are the requirements to enable system managed rebuild and the ALTER command for the Coupling Facility structure used by CA TPX?

A: All instances of CA TPX connected to the structure must be r5.3 or r5.4. The operating system and CFLEVEL must support this functionality.

Q: When signing on, I get message IENS008A (THE SECURITY SYSTEM IS INACTIVE), but RACF is active. What is wrong?

A: CA TPX has called RACF to validate the user ID and password submitted during signon. An abend occurred in RACF processing that was percolated up to CA TPX. CA TPX recovers from the abend and indicates the external security system is unavailable. This condition should be reviewed. It is likely that the security file was locked at the time and normal processing will resume when the condition is cleared. If it becomes necessary to obtain a dump of this condition, a SLIP trap should be set for the appropriate abend code with the address spaces to be dumped.

Q: Do I need to code the new switch-in exit (TPXUSWIN)? CA TPX successfully refreshed the screen in my shop.

A: You do not need to code the exit. CA TPX will use the current methods (that is, those used in r5) to refresh the screen image. The exit is intended for those applications that make heavy use of graphics and have the capability of refreshing the screen image on their own.

Q: Qualified pass ticket works when my application is running on the same instance of the operating system as CA TPX, but if I move it to another instance, the logons are rejected by the application. What did I do wrong?

A: The pass ticket profile in the external security system used for pass ticket generation and validation for any given application must be identical. When security systems do not share the same security database, a mismatch can occur resulting in a validation failure for a good ticket.

Q: Can CA TPX use qualified pass tickets when RACF is the security system on the operating system image on which the target application resides?

A: Yes. To generate qualified pass tickets, CA TPX requires CA Top Secret or CA ACF2 to be the active security system on the operating system image on which CA TPX is active. An appropriate pass ticket profile must be defined to the eTrust solution. When the appropriate pass ticket profile is defined to RACF for an application, RACF can interpret a qualified pass ticket generated by CA TPX in conjunction with one of the previous eTrust solutions.

Q: I already have a TN3270 Server from a vendor other than CA. Can CA TPX communicate directly with that server?

A: No. CA developed a high-speed protocol between CA TPX and TCPaccess Telnet Server to provide the fastest means with the least overhead for transferring data between the solutions and moving the data to its final destination. CA TPX can use standard VTAM LU0 or LU2 sessions to communicate with TN3270 servers from other vendors.

Appendix A: VSAM File Sharing Without CA-L-Serv

This appendix describes VSAM file sharing managed directly by CA TPX and the required setup procedure.

This section contains the following topics:

How It Works

In CA TPX, the VSAM data sets are shared by setting VSAM share options to (4,3). ENQ/DEQ logic manages the sharing process.

The ENQ uses a RESERVE to serialize access to the VSAM data sets. The qname of this ENQ is TPXMS. If the VSAM data set is cataloged in an ICF catalog, the rname is the name of the data set. If the VSAM data set is not cataloged, the rname is the data definition name, ADMIN1, ADMIN2, MAIL, NOTES, or VIEW. Testing has shown that converting the RESERVE using a product such as CA MII is not necessary and increases the overhead associated with the cross-system sharing process.

Important! The overhead associated with this serialization causes considerably higher I/O rates to the VSAM data sets.

Sharing information about each VSAM data set is maintained in record zero of the data set (the key consists of 17 “0”s). The VSAM shared information (VSI) for the Data and Index data sets is written to record zero to pass the information cross-system. If any VSAM data set is restored or moved, the information in control record zero becomes inaccurate, so it must be deleted. You can use batch administration to delete control record zero. For more information, see the *Batch Administration Guide*.

If a VSAM data set is coded as DISP=SHR in the DD statement in the startup procedure, that data set will be shared.

Allow VSAM Sharing Without CA-L-Serv

To allow VSAM sharing in your system

1. Set the VSAM share options on each VSAM data set to (4,3).
2. Specify DISP=SHR in the DD statement for any data set that is to be shared.
3. Re-evaluate your usage of the option Reserve ACB's at startup on the Performance Parameters panel in the System Options Table (SMRT). If it is set to Y, startup will be slowed down significantly when VSAM sharing is used.

   The option Reserve ACB's at startup causes the product to read the entire ADMIN2 data set, searching for user records that have ACB names that are fully qualified (consist of eight characters and no masks). With VSAM sharing this process is slow.

   You must set this option to Y only if you have assigned users a fully qualified ACB name through User Administration. If you have assigned users by using masking, the Reserve ACB's at startup option can be set to N.

   If you must reserve specific ACBs for specific users, in most cases you can set up masking rules to accomplish this. If you cannot use masking, using either the ACB Selection Exit or the OPENGATE feature can eliminate the need for using the Reserve ACB's at startup option.
4. Authorize the load library on each system that CA TPX runs on.
5. Re-evaluate the placement of the VSAM data sets. You can move them to minimize the effects of the RESERVEs used to serialize access to the data sets.

Note: Sharing is not possible for VM systems or non-authorized copies of this product. If you select sharing and do not authorize CA TPX, an abend will occur.

Appendix B: VSAM File Sharing With CA-L-Serv

This appendix briefly discusses CA-L-Serv and explains how to customize CA TPX and CA-L-Serv to allow CA-L-Serv to manage CA TPX VSAM files.

Note: For detailed information on CA-L-Serv, see the CCS for z/OS documentation.

This section contains the following topics:

CA-L-Serv Benefits

CA-L-Serv is a master started task that provides standard services used by many CA products.

CA-L-Serv can simplify VSAM file sharing for different combinations of CA TPX on one or more z/OS systems. CA-L-Serv can:

- Provide easier cross-system VSAM file sharing among multiple copies of CA TPX operating on different systems.
- Improve file security by establishing CA-L-Serv as the only user that can access the VSAM files.
- Provide a log containing the key of each VSAM record that has been updated through CA-L-Serv.
- Provide less disruptive backup and restore operations by allowing maintenance on individual VSAM files without taking down CA TPX.

File Sharing With CA-L-Serv

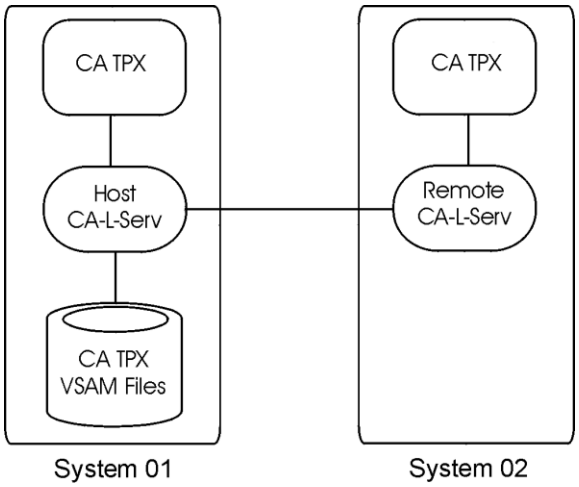
When using CA-L-Serv, CA TPX accesses the VSAM files through the CA-L-Serv file server component. Only CA-L-Serv has direct access to the files. It takes read and write requests from CA TPX and determines the correct VSAM file to access.

Control record zero, which contains VSAM sharing information when CA-L-Serv is not used, is deleted when the VSAM files are opened for update.

CA-L-Serv Cross-system Sharing

With CA-L-Serv managing the files, you can share VSAM files across systems, even when shared DASD is not available. In this case, CA-L-Serv must exist on each system with the communications server providing cross-system communication.

A single CA-L-Serv, defined as the *host*, manages the VSAM files, while the other CA-L-Servs are defined as *remote*, as in the following illustration:



Note: If your site is using one CA-L-Serv on one system, the CA-L-Serv must be defined as *local*.

If CA-L-Serv Becomes Unavailable

CA TPX will detect when CA-L-Serv or any of the files managed by CA-L-Serv cannot be accessed. CA TPX will mark the affected files as unavailable and periodically attempt to access them.

The period between attempts is the CA-L-Serv Recovery Retry Interval. The default interval is 120 seconds. You can set the interval in the System Options Table (SMRT) after CA TPX has been installed and started.

When the files become available, the CA TPX accesses them and marks them available.

You can determine the status of the VSAM files by issuing the D FILES command in a TPXOPER session.

How to Customize CA TPX

This section explains how to customize the CA TPX startup procedure to allow VSAM file sharing with CA-L-Serv.

Omit DD Statements

If you want TPX to access a VSAM file through CA-L-Serv, omit the DD statement for that file from the CA TPX startup procedure.

Identify CA-L-Serv to CA TPX

CA TPX must recognize the CA-L-Serv subsystem name to establish communication. To identify the subsystem name to the product, place the following statement in the startup procedure:

```
//SSN$name DD DUMMY
```

The default subsystem name is LSRV. The subsystem name is assigned to CA-L-Serv when CA-L-Serv is installed.

Specify the DDname Prefix

You must specify a DD statement in the startup procedure to specify the CA-L-Serv ddname prefix. The prefix is a four-letter code. The VSAM files are defined to CA-L-Serv with the same prefix. CA-L-Serv allows CA TPX to access files with the matching prefix. Different copies of CA TPX can use different prefixes, which allows CA-L-Serv to control the sharing of different file sets concurrently.

Place the following statement in the startup procedure to define the prefix:

```
//DDN$prefix DD DUMMY
```

By specifying the same prefix in the startup procedure of another CA TPX, both copies will share the same VSAM files.

Specify the ICSN

You can include an ICSN= statement in the JCL EXEC parameters indicating the intercommunications system name of CA TPX. CA-L-Serv uses this name to identify this copy.

The default ICSN is the started-task name.

How to Customize CA-L-Serv for CA TPX

This section explains how to customize CA-L-Serv to manage the CA TPX VSAM files.

You must modify the startup procedure to specify which files are being managed by which CA-L-Serv.

Also, you must structure the CA-L-Serv parameter data sets, which contain members that provide operating values to CA-L-Serv and issue CA-L-Serv commands.

Specify the Files CA-L-Serv Manages

You must specify to CA-L-Serv the VSAM files it is managing.

Use the ddname prefix, as described in Specify the DDname Prefix (see page 73), to identify which files will be accessed by each CA TPX instance.

For example, use the following ddnames for the VSAM files if you are using the ddname prefix **TPXV**:

```
TPXVADM1
TPXVADM2
TPXVNOTE
TPXVMAIL
TPXVVIEW
```

When using CA-L-Serv to manage file sharing, you must ensure that CA-L-Serv is the *only* address space with update access to the files. To ensure adequate protection, you must carry out the tasks described in the following paragraphs.

Specify the Disposition and Share Options

To ensure adequate protection for the files, you must carry out the following tasks:

- Set the VSAM share options for managed files to (1,3) or (2,3). This takes advantage of CA-L-Serv performance advantages and is required to ensure restricted access to the managed files.
- Set the VSAM option for managed files to REUSE.
- Set the disposition of managed files to DISP=OLD in the CA-L-Serv startup procedure.

To do this, override the default (DISP=SHR) using the following steps:

1. Code a DD statement explicitly for the file in the CA-L-Serv startup JCL.
2. Code the ADDFILE command for the file with the ddname but *without* the data set name.

Unless you perform these steps, the ADDFILE command will allocate the file with DISP=SHR, and the file can be exposed to unauthorized updates.

When a file is allocated with DISP=OLD, it cannot be browsed online while under CA-L-Serv management, and the CA-L-Serv IFSYS command cannot be used to run multiple copies of CA-L-Serv with the same initialization commands and startup procedures. Using the IFSYS command in this manner would cause the multiple copies of CA-L-Serv to attempt to allocate the same files with DISP=OLD.

Propagate ENQs

The following ENQs must be propagated across all systems that share the DASD on which the managed files reside:

- The LSERVDSN ENQ. This is issued by CA-L-Serv against a VSAM file when the file is placed under CA-L-Serv management with an ADDFILE command. This ENQ is used to determine whether CA-L-Serv is managing the file.
- The SYSVSAM ENQ. This is issued by VSAM when a VSAM OPEN takes place. Share options of (1,3) or (2,3) use this ENQ to restrict update access to the file.
- The SYSDSN ENQ. This is issued by z/OS when an OPEN takes place against a data set that is coded DISP=OLD.

You can use a product that propagates ENQ requests globally, such as CA MII Data Sharing. Your site probably already has methods to propagate the SYSVSAM and SYSDSN ENQs.

Use Private Buffer Pools

We recommend that you use private buffer pools. Private buffer pools are used by default-you do not have to specifically assign files to them. Do not use local shared resource (LSR) buffer pools.

Sample Members

The CB0VJCL data set includes the following members that pertain to CA-L-Serv:

LSVTPX

CA-L-Serv startup commands for CA-L-Serv managed access to all VSAM files for the component of CA TPX.

LSVNVIMG

CA-L-Serv log messages indicating the beginning and end of sessions with CA-L-Serv.

Installation Checklist

The following tables provide a checklist for installing and customizing the CA-L-Serv and the CA TPX components:

General	Completed
VSAM files that are managed by CA-L-Serv are managed by a single CA-L-Serv.	
Each VSAM file is accessed through CA-L-Serv or directly by TPX, but not both.	
Implement a security package to restrict access to the VSAM files.	
Ensure that the LSERVDSN, SYSVSAM, and SYSDSN ENQs are propagated as necessary.	

CA-L-Serv Installation	Completed
CA-L-Serv startup parameters match those in sample CA-L-Serv startup members, after any required customization for your site.	
The CA-L-Serv that is managing the product files is defined as *host* if you are cross-system sharing or *local* if you are not.	
All CA-L-Servs defined as remote have the same z/OS subsystem name as the host CA-L-Serv	
The CA-L-Serv file server is active on each CA-L-Serv system.	
If your site is performing file sharing with more than one CA-L-Serv, the CA-L-Serv communications server is active on each CA-L-Serv system.	
Each CA-L-Serv communication server has the correct VTAM applid.	

CA-L-Serv Installation	Completed
All VSAM files that are managed by CA-L-Serv have VSAM sharing options of (1,3) or (2,3).	
An ADDFILE command is present for each file that CA-L-Serv is managing.	
Each file that CA-L-Serv is managing has a DD statement specifying DISP=OLD in the startup procedure of the local or host CA-L-Serv.	

CA TPX Startup Procedure	Completed
The CA-L-Serv subsystem name specified in the startup procedure matches that of the CA-L-Serv system with which the product must communicate.	
The ddname prefix specified in the startup procedure matches that used in the CA-L-Serv ADDFILE commands.	
A DD statement is present for each VSAM file that is to be accessed directly by TPX	
.The Intercommunications System Name (ICSN), which identifies each component to CA-L-Serv, is correct.	

Appendix C: APPL Statements

This chapter describes the APPL statements contained in the TPXAPPL member.

This section contains the following topics:

Primary APPL Statement

This is the primary APPL statement:

```
TPX APPL AUTH=(ACQ,PASS),MODETAB=TPXLGMOD. . .
```

This statement identifies a primary logical unit (PLU) named TPX. A PLU is the application that your 3270-type terminals communicate with directly. Each product installed at your site must have a different name on its primary APPL statement.

Rebind APPL Statement

This is the rebind APPL statement:

```
TPXRBIND APPL AUTH=(ACQ,PASS),MODETAB=TPXLGMOD. . .
```

This statement identifies an ACB that the product uses to perform a rebind function that has been specified either by a user exit or by a terminal options table parameter. Using an extra ACB for the rebind process allows the product to rebind to connections that disconnect immediately upon receiving an UNBIND (such as TCP/IP connections).

APPL Statements for Shared Virtual Terminals

This is the APPL statements for shared virtual terminals:

```
TPXSHARE APPL MODETAB=TPXLGMOD,DLOGMOD=T3278M2. . .
```

This statement identifies a parallel secondary logical unit (SLU) named TPXSHARE. It can be used for applications such as TSO that can communicate with many different users who share one virtual terminal.

Note: This statement is not used in PASS mode.

If the product is connecting to an application using its VTAM generic name, the TPXSHARE APPL should not be used. VTAM routes all sessions with a particular generic resource to the same instance of that application. We recommend that you use Group Virtual terminals as defined next.

APPL Statements for Group Virtual Terminals

These are the APPL statements for group virtual terminals:

```
TPXGR001 APPL MODETAB=TPXLGMD2,DLOGMOD=T3278M2. . .
TPXGR002 APPL MODETAB=TPXLGMD2,DLOGMOD=T3278M2. . .
         .
         .
         .
TPXGR020 APPL MODETAB=TPXLGMD5,DLOGMOD=T3278M5. . .
```

These statements identify the virtual terminals TPXGR001 through TPXGR020, each of which is an identical, *non-parallel* SLU. The product uses these statements for applications such as IMS and CICS, which can have many different users but permit only limited sharing of virtual terminals. With these applications, a virtual terminal can establish only one session with a particular application (for example, CICS). However, that virtual terminal can be shared by a group of users, as long as the users are accessing different applications through that terminal.

Note: These statements are not used in PASS mode.

APPL Statements for Unique Virtual Terminals

These are the APPL statements for unique virtual terminals:

```
TPXUN001 APPL MODETAB=TPXLGMD2,DLOGMOD=T3278M2. . .
TPXUN002 APPL MODETAB=TPXLGMD2,DLOGMOD=T3278M2. . . . . .
         .
         .
         .
TPXUN020 APPL MODETAB=TPXLGMD2,DLOGMOD=T3278M5. . .
```

These statements identify the virtual terminals TPXUN001 through TPXUN020. Each of these can support a single session between one user and one application; it cannot be shared among several applications or users.

Any application that is not predefined in the Application Characteristics Table (ACT) must use one of these virtual terminals exclusively.

Note: These statements are not used in PASS mode.

Important! If you access the IBM Information Network, you must make your virtual terminal LU names unique for your site.

APPL Statements for Application Passthrough Printing

These are the APPL statements for application passthrough printing:

```
TPXAP001 APPL MODETAB=TPXLGMOD,DLOGMOD=PLU1TPX. . .
TPXAP002 APPL MODETAB=TPXLGMOD,DLOGMOD=PLU3M2. . .
         .
         .
         .
TPXAP006 APPL MODETAB=TPXLGMOD,DLOGMOD=PLU0M2. . .
```

These statements identify the virtual printers TPXAP001 through TPXAP006, used for Application Passthrough Printer Support (APPL PPS). For APPL PPS, you associate a pool of real printers with a virtual printer.

APPL Statements for User Passthrough Printing

These are the APPL statements for user passthrough printings:

```
TPXUP001 APPL MODETAB=TPXLGMOD,DLOGMOD=PLU1TPX. . .
TPXUP002 APPL MODETAB=TPXLGMOD,DLOGMOD=PLU3M2. . .
         .
         .
         .
TPXUP006 APPL MODETAB=TPXLGMD5,DLOGMOD=PLU0M2. . .
```

These statements identify the virtual printers TPXUP001 through TPXUP006. The product uses these statements for User Passthrough Printer Support (USER PPS). For USER PPS, you associate a virtual printer with the virtual terminal from which the user requested a print function.

Appendix D: Data Set Name Changes

This Appendix describes the name changes of the data sets starting in release 5.3 of CA TPX.

This section contains the following topics:

New Data Set Names

New Name	Old Name	RELFILE	Description
CB0VDATV	N/A	CB0V530.F6	Unloaded VSAM files
CB0VJCL	INSTALL	CB0V530.F4	Post installation jobs and samples
CB0VLOAD	LOADLIB	CB0V530.F1	The distributed object modules
CB0VMAC	GENLIB	CB0V530.F2	TPX macros available for user exits
CB0VPDAN	PANELDA	CB0V534.F1	HDA… & TDA… panels
CB0VPDES	PANELSG	CB0V53D.F1	HSG… & TSG… panels
CB0VPDEU	PANELGE	CB0V538.F1	HGE… & TGE… panels
CB0VPENP	PANELUP	CB0V53G.F1	HUP… & TUP… panels
CB0VPENU	PANELEN/PANELCU	CB0V531.F1	HCU… , HEN… , TCU… & TEN… panels
CB0VPESP	PANELSP	CB0V53E.F1	HSP… & TSP… panels
CB0VPFIN	PANELFI	CB0V536.F1	HFI… & TFI… panels
CB0VPFRA	PANELFR	CB0V537.F1	HFR… & TFR… panels
CB0VPFRB	PANELBF	CB0V532.F1	HBF… & TBF… panels
CB0VPFRS	PANELSF	CB0V53C.F1	HSF… & TSF… panels
CB0VPITA	PANELIT	CB0V539.F1	HIT… & TIT… panels
CB0VPJPN	PANELJP	CB0V53A.F1	HKA… & TKA… panels
CB0VPNLD	PANELDU	CB0V535.F1	HDU… & TDU… panels
CB0VPNOR	PANELNO	CB0V53B.F1	HNO… & TNO… panels
CB0VPPTB	PANELBP	CB0V533.F1	HBP… & TBP… panels
CB0VPSVE	PANELSW	CB0V53F.F1	HSW… & TSW… panels

New Name	Old Name	RELFILE	Description
CB0VSCRI	ACLLIB	CB0V530.F3	Supplied ACL/E scripts
CB0VSRC	SAMPLIB	CB0V530.F5	Sample exits and more
SAMPJCL	N/A	SAMPJCL	Jobs to install the product

Index

S

T

U

V